Page 3, before line 1, insert the following heading:

--**Summary of the Invention** --.

Page 4, before line 1, insert the heading:

--**Brief Description of the Drawing**--;

between lines 17 and 18, insert the heading:

--**Detailed Description**--.

IN THE CLAIMS:

1. (Amended) A system of managing the security of data processing applications, [characterised in that] comprising:

[-] directory files in which the data processing applications are stored, said [recorded in] directory files [(Repl, Rep2, Rep3l, Rep32, Rep4l, Rep42, Rep5l, Rep52)] being organised in an n-level tree, the level 1 directory [(Repl)] being the highest level ; and

[-] a number [r] of security registers [(R)] which can each be allocated to a single directory [and], each security register [(R)] containing all the rights or secrets [Sl to Sp] which have been granted under a directory.

2. (Amended) A method of managing the security of data processing applications [in a system according to Claim 1, characterised in that it comprises the following steps consisting], comprising the steps of :

(a) storing in security registers [(R)] the rights [(Sl to Sp)] granted under a directory [(Rep)] according to given rules [(RG1, RG2, RG3)];

A2

(b) seeking [in the tree] the secrets presented in an n-level tree of directory files in which data processing applications are stored; and

(c) verifying the knowledge of one or more rights at the level of the data processing application.

3. (Amended) A method according to Claim 2, [characterised in that] wherein the storage rules of step (a) are as follows :

[(RGI) :] allocation of a security register [(R)] to [the] a current directory as soon as a right has been granted under this directory or [the] said security register has been updated if a right has already been granted under this directory ;

[(RG2)] loss of the link connecting the old current directory to its security register when a new directory is selected except if the selected directory is the child of the old current directory; and

[(RG3)] allocating the security register that was allocated the earliest to the new current directory if the security registers are all allocated.

4. (Amended) A method according to Claim 2 [or 3, characterised in that] wherein step (b) consists of applying the following rule [consisting of]:

[(RG4)] verifying that the secret presented [(S)] is known in the current directory (Ni) or in a directory at a higher level.

5. (Amended) A method according to Claim 2, [3 or 4, characterised in that] wherein step (b) comprises the following intermediate steps [consisting of]:

A2

(bl) seeking a secret in the current directory at level (Ni) and verifying the existence of the secret [(S)] within the application ;

(b2) if [this] said secret [(S)] exists, verifying that the presentation of the secret has succeeded ;

if the presentation has succeeded, the right associated with the secret [(S)] is granted at the level (Ni) of the current application ;

if the presentation has failed, the right associated with the secret [(S)] is not granted and the attempted presentation is terminated ;

(b3) if [this] said secret [(S)] does not exist within the current application at level (Ni) , seeking whether this secret [(S)] exists within the parent application at level N(i-1) ;

(b4) if [this] said secret [(S)] exists in the parent application at level [B]N(i-1), verifying that the presentation has succeeded ;

if the presentation has succeeded, the right associated with the secret [(S)] is granted in the current application at level (Ni) ;

if the presentation has failed, the right associated with the secret [(S)] is not granted and the attempted presentation is terminated ;

(b5) if the secret does not exist within the parent application at level N(i-1), seeking the existence of the secret [(S)] at the level of the application at level N(i-2) along the hierarchical axis and verifying that the presentation has succeeded ;

and so on as far as the highest hierarchical level as long as the existence of the secret [(S)] has not been discovered ;

(b6) if the secret [(S)] has not been discovered, the attempted presentation is terminated.

6. (Amended) A method according to [one of the preceding Claims 2 to 5, characterised in that] claim 2, wherein the step (c) consists of applying the following rule [consisting of]:

[(RG5)] authorisation of a function requiring knowledge of a secret [(S)] if and only if, running through the tree along the hierarchical axis from the current application to the root application, the first secret [(S)] is known to at least one of the applications belonging to the tree section for which the current application and the application containing the secret [(S)] are delimiters.

7. (Amended) A method according to [one of the preceding Claims 1 to 6, characterised in that] claim 2, wherein step (c) comprises the following steps [consisting of]:

(c1) verifying that a security register is associated with the current application at level Ni ;

(c2) authorising the function if the security register contains the required right and terminating the verification ;

(c3) seeking the existence of the reference secret [S] within the current application at level Ni if no security register is associated with the current application or if the associated register does not contain the required right ;

(c4) refusing the function and terminating the verification if the secret exists within the current application;

(c5) verifying that a security register is associated with the parent application at level N(i-1) of the current application if the reference secret [S] does not exist within the current application at level Ni;

(c6) authorising the function and terminating the verification if the security register associated with the parent application contains the right required for using the function ;

(c7) seeking the existence of the reference secret [S] within the parent application at level N(i-1) of the current application if no security register is associated with the parent application or if the associated security register does not contain the required right;

(c8) refusing the function and terminating the verification if the reference secret [S] exists within the parent application at level N(i-1);

(c9) verifying that a security register is associated with the grandparent application at level N(i-2) of the current application along the hierarchical axis of the current application towards the root application, if the reference secret [S] does not exist within the parent application at level N(i-1);

and so on as long as the existence of the reference secret [S] has not been discovered;